DIGITAL EVIDENCE FROM THE INTERNET AND THE CLOUD

Krunoslav Antoliš, PhD
Police Academy, Zagreb, Croatia

Abstract: In the modern world, the use of ICT communication technologies has become an integral part of life. ICT Infrastructure is the bearer of digital traces of overall legitimate and illegal activities that are through it an unavoidable source of digital evidence. However, in order to prove something, it must also obtain the law as envisaged by the law of an authorized person. The legal norm thus defined is not a problem in the analog world, but it is a big problem when it comes to the virtual world. Namely, the virtual infrastructure, especially the Internet and the new challenges that the cloud architecture brings to us, because of its physical positioning outside the state borders, questions the legality of search and collection. Within this paper, the legal bases for handling the virtual space at the international level are analyzed, such as the Council of Europe Cybercrime Convention, the US CLOUD Act, Australian Decryption Bill and GDPR. The article's intent is to support decision-makers in taking clear national positions regarding the aforementioned legal norms and their mutual interaction. The paper compares the legal consequences of such behavior and the acceptability of such digital evidence collected and possible violation of the privacy of legal and natural persons!

Keywords: Digital Evidence, Virtual Infrastructure, Legal Standards, Internet, Cloud.

INTRODUCTION

At present, evidence of crimes is increasingly being collected by smartphones, gadgets, IOTs, the Internet and the cloud. This is also the main reason why digital evidence has become essential in almost all criminal investigations. But that does not mean that gathering such evidence is simple and effortless. Law enforcement agencies are faced, among other things, with two major challenges in their investigations, namely: jurisdiction and encryption.

Effective criminal investigations often depend on whether a country conducting an investigation is authorized under its domestic law to obtain electronic data held by ISPs' Internet service providers under its authority, including their affiliates outside state borders.

The competence of national legal frameworks is limited to a certain state territory, while our communication and use of data, due to the Internet, cloud computing and technological development, is one that does not know the state borders. A provider of communication and cloud computing platforms such as Skype, WhatsApp, Microsoft, Google and Dropbox will more often than not store data in the country where the user resides, thus depriving the national legal system of its ability to legally act.

Communication service providers who often have electronic evidence of certain criminal acts can have clients around the world, and business offices and data storage facilities in many different countries. As a result, ISPs and data controlled may be subject to the laws of multiple states. Conflicting legal obligations can arise when an ISP receives an order from a government that requires disclosure, but the rest of the government restricts the disclosure of these same information, although they may be vital for timely and effective criminal investigations.

VARIOUS APPROACHES

Lawmakers responded to these challenges by introducing new legal solutions, and examples of these solutions were: The Bill on Clarifying Legitimate Data Use Rights (CLOUD Act), Australian Decryption Bill, Council of Europe Cybercrime Convention, GDPR - which cares about privacy on electronic infrastructures, as well as many others. It is often neglected by the public that the consequences and dilemmas that providers of ISP services might face with criminal reports due to non-compliance with legal frameworks, because the penalties are large. For example, for non-compliance with the EU General Data Protection (GDPR) regulation up to EUR 20 000 000 or 4% of the total annual worldwide turnover of the previous financial year.

ACCESS TO THE PROBLEM BCOUNCIL OF EUROPE CYBERCRIME CONVENTION

The Cybercrime Convention (also called the "Budapest Convention") requires each of the more than 60 countries that the signatories of the agreement have to retain the statutory power to compel companies in their area to disclose the stored electronic information under their control in accordance with the applicable legal process, without exception to the information that the company sells in another country.

Article 18 (1) (a) of the Budapest Convention obliges each Party to "adopt legislative and other measures that may be necessary to enable its competent authorities to order a person in its territory to supply certain computer data in the possession of that person or control, which is stored in a computer system or a storage medium for computer data. "

However, ISPs may also be subject to the laws of other countries that restrict the disclosure of certain types of data, either because the data is stored in another country or require action in another country to disclose them, or because the data relate to other nationals country.

If national laws are in conflict, civil servants may be forced to choose which country's laws will follow, knowing that they can face the consequences of violating the law of another country. Such conflicts pose serious problems for government-seeking data and may hinder important investigations.

Sometimes such conflicts of law problems can be solved by submitting a request for "mutual legal assistance" to another country, using a system of agreements called "Mutual Legal Aid Treaty" (MLATs), but this process has many steps and depending on country and complexity may take several months. This is certainly one of the reasons why "Mutual Legal Assistance (MLA) is generally considered ineffective and accentuated in relation to obtaining electronic evidence, as the binding time is a response to the requirements of the six to 24 months standard. Many requests and thus investigations are abandoned. This negatively affects the government's positive commitment to protecting society and individuals from cybercrime and other criminal acts involving electronic evidence.

In order to overcome the challenge of jurisdiction and speed up the investigation process, local authorities have started searching for information relevant to their criminal investigations over the past few years, directly from service providers, regardless of the location of the data, and some countries also adopted regulations that make such a process legitimate.

ACCESS TO THE PROBLEM CLOUD ACT

One, if not the most prominent instance where the required data is stored on foreign-site servers, is Microsoft Ireland. The case began in December 2013, when the US court ordered Microsoft to surrender data belonging to Microsoft's email account in Ireland. The service provider disputed a court order based on arguments on jurisdiction and sovereignty, resulting in a legal battle between the Ministry of Justice (DOJ) and Microsoft, which ended before the Supreme Court in 2017.

However, before the Supreme Court could decide on this issue, in March 2018, the US Congress passed the CLOUD Act, which now allows American LEAs to request data from US service providers even if these data are stored on servers abroad.

The United States has passed the CLOUD Act, which accelerates access to electronic information held by global ISP providers based in the United States.

Law on Clarification of Legitimate Overseas Data Use Law or the "Law on Clouds". The Law on Clouds allows the United States to conclude executive agreements with other countries that meet certain criteria, such as respect for the rule

of law, in solving the problem of conflict of law. For investigations of serious criminal offenses, ISPs may qualify for qualified, legitimate electronic data orders issued by another country.

The CLOUD Act explicitly states in US law the long established US and international principle that a company under the jurisdiction of a country may require to deliver the information the company controls, no matter where it is stored at any time. The CLOUD requires that CSPs subject to US jurisdiction must disclose information that corresponds to the lawful US legal code, no matter where the company stores the data.

CLOUD requires that foreign governments' orders subject to an executive agreement should not deliberately target individuals or individuals in the US in the United States. The foreign government is free in negotiations to look for similar restrictions that would prevent the United States from using orders subject to an agreement to target its citizens or residents. The US and other countries may continue to use their existing legal process to search for data outside the CLOUD law, but under such circumstances they may still face a conflict of laws.

At the same time, the court proceedings required by a lawsuit requesting State under the CLOUD Act do not have to comply with legal requirements in the United States. Instead, judicial proceedings must comply with the requirements of domestic law for the information requested.

When acting under the CLOUD Act, foreign bodies may use their domestic legal procedures directly to service providers in accordance with their own law, and service providers may disclose responsible information directly to foreign authorities.

The CLOUD Act has not changed or extended the historical scope of orders issued under US law, i.e. random or bulk data collection is not permitted.

The CLOUD Act is applied in accordance with the following definitions: 18 U.S.C. § 2510 (15) ("electronic communications service" means any service that provides users with the ability to send or receive wire or electronic communications); identity card. § 2711 (2) ("Remote Computer Services" means the provision of computer storage and data processing services through the electronic communications system of the public).

These definitions include companies such as email service providers, mobile phone companies, social media platforms, and cloud storage services. They do not include a business just because they have some interaction with the Internet, like certain e-commerce sites.

These definitions are in accordance with Article 1c. Budapest Convention, which includes "any public or private entity that provides its users with the possibility of communicating via a computer system" and "any other subject that processes or stores computer data on behalf of such a communication service or user of such service."

Even if LEAs gain access to data, for example, either by downloading a mobile phone or by requesting data from providers, the increasing popularity of encryption technology prevents LEAs from understanding the data. Data in encrypted format only detects encrypted information.

An example of real life should help to better understand these challenges. The Federal Judge asked Apple to assist the Federal Bureau of Investigation in providing reasonable technical assistance to unlock the encrypted iPhone, which belonged to San Bernardo's terrorist shooter since December 2015. Apple has refused, fearing that such assistance would could set a precedent and hurt the security of encryption technology in the coming years. Finally, the FBI managed to unlock the iPhone without Apple's help, which is why the case did not continue.

Another example relates to encrypted communication. In a two-year investigation that was alive to the media, in 2013, the FBI removed the Black Market Silk Road forum, which allowed drug trafficking and other inadequate goods online. The Silk Road owed its success to a combination of anonymity and encryption. It was a hidden service in Darknet, a network of computers using a cryptographic communications protocol, making it difficult to enforce laws to locate a site server, its administrators, and its users. Finally, the server, at which time it was a party, was in Iceland and confiscated after a successful US mutual legal assistance request.

ACCESS TO THE PROBLEM IN AUSTRALIAN "DECRYPTION" BILL

Australia already has laws that require service providers to file information to the suspect police, but the issue with encrypted messages now is coming. Deciphering is possible if the service provider uses a form of encryption that allows them to view the user's message. But in recent years, services such as WhatsApp, Signal, etc., adding an additional layer of security known as end-to-end encryption, disable decryption, which even the FBI admits is a big problem.

Because end-to-end encryption only allows the sender and receiver to view the message, preventing it from decrypting the service provider.

Australia and other countries say terrorists and criminals exploit this technology to avoid surveillance.

On the other hand, Australian lawmakers have now decided to ensure that national security and law enforcement agencies have the modern tools they need, with appropriate powers and oversight, to access encrypted conversations of those who want to do harm, by granting the Assistance Act and access only recently 6 December 2018. The Australian Law on Telecommunication Access and Assistance allows the government to foster cooperation and capabilities from companies such as social media companies, telecommunications, manufacturers, or even any retail company that provides its customers with WiFi. The law will

force technology companies to help Australian governments decipher network users' communications - and this could be a big blow to privacy in other parts of the world. The law provides for up to $ 7.3m for corporations as well as jail.

Privacy agents fear that the bill could have implications for other countries such as the United Kingdom or the United States. But such exploratory powers are necessary in the light of the above-mentioned examples, however, the obligation to create a backdoor for "good guys" will ultimately lead to the weakening of security measures that "bad guys" can also take advantage of CLOUD does not require service providers to decrypt data in response to law enforcement requirements. The CLOUD law is "neutral encoding". It does not create any new law enforcement authority to force service providers to decrypt communications. It neither prevents service providers from assisting in such deciphering or preventing countries from addressing decoding requests in their domestic laws.

PRIVACY POLICY GDPR VS CLOUD ACT

Privacy concerns created by GDPR on EU territory in the application of CLOUD law are also reflected in the fact that ISP service providers can notify search account owners in accordance with the US court's order under the Law on Preserved Communications unless an independent judge has issued a security order. Protective orders pertaining to all provisions of the Act on Preserved Communications (and not just orders in accordance with the CLOUD Act) shall be issued when the Independent Judge finds that there is reason to believe that a notification of a court order may result in adverse outcome (1) physical security of an individual; (2) escape from persecution; (3) Destruction or manipulation of evidence; (4) intimidation of potential witnesses; or (5) otherwise seriously endangers the investigation or unjustifiably delayed the trial. In accordance with the US Department of Justice's policy, such orders must in general be limited to one year.

In the modern world, the use of information and communication technologies - ICT has become an integral part of life. ICT infrastructure is the bearer of digital traces of all legitimate and illegal activities that through it are inevitable sources of digital evidence. However, in order to prove something, it must also obtain the law provided for by the law of the authorized person. The so-defined legal norm is not a problem in the analog world, but it is a big problem when it comes to the virtual world. Namely, the virtual infrastructure, especially the Internet and the new challenges that cloud architecture brings to us because of its physical positioning outside the state borders, challenges the legality of search and collection.

DIGITAL EVIDENCE ON THE CLOUD

Cloud computing as part of ICT is a paradigm of information technology (IT) that describes the provision of IT infrastructure such as storage space or application software as an Internet service. Technically, it describes the access to IT infrastructure that is available through a computer network without the need for installation on a computer.

The most interesting cloud service model is certainly an electronic (digital) proof of service database service model (DbaaS). Users can access database without the need to install physical hardware and software. Maintenance and administrative services are performed by the service provider while the user pays the service using that database. Looking at the security aspect of the data, the user who stores the Cloud data protection data is transferred to the service provider, while reducing the control over that data. It is very complicated when such providers are out of reach of domestic legislation, which in many cases is the rule because servers of such clouds can be anywhere in the world.

Investigators of this kind of crime are a major obstacle to "protecting personal data" and the obligation to keep such data on a server that regulates GDPR. A legal conclusion regarding the definition of public, private, personal and all other types of data circulating on the Internet is the protection of even what could be used as electronic (digital) evidence. Three types of data can be interesting for the purposes of criminal investigations: subscriber data, traffic data and so-called content data.

ACCESS TO THE PROBLEM NATO APPROACH

NATO also supported "Improved cyber defense policy", based on its cyber defense policy in 2011. In a statement accompanying the meeting of heads of state, NATO confirmed that "international law, including international humanitarian law and the UN Charter, applies in cyberspace" and clarified that "the North Atlantic Council will decide when cyber attack will bring to refer to Article 5 [governing the collective defense] ".

Contrary to the potential consensus that is developing on cybercrime, disputes over cyber security and sovereignty issues are more fundamental and less likely to make wider international agreements. The Chinese and Russian "Information Security" concept suggests that they advocate a governance model that is geared to sovereignty, which is opposed to the multiple-access, bottom-up approach advocated by the United States and the European states. Regional agreements establishing these fundamentally different approaches are likely to be barriers rather than step-by-step steps for wider future agreements. However, regional agreements such as NATO's declaration can provide useful clarity as to how individual countries and their allies see specific behavior in cyberspace and how they will respond to cyber security incidents. In other words, although conflicting regional

agreements can not encourage a broader agreement, they can at least help to promote clarity and conflict avoidance.

COUNCIL OF EUROPE CYBERCRIME CONVENTION RUSSIA, CHINA, INDIA

Whether a comprehensive international treaty is needed that could also cover the crime and behavior of the state in the cyber space is one of the major issues related to cyber security with which the international system is currently facing. Some have argued that it is just now impossible to negotiate even a limited-scope agreement on the Cybercrime Convention at a global level - the differences in opinions about what constitutes the corresponding global standards are simply too big, it is claimed that it is particularly difficult to extend the process and collaborative obligations to global level. At the same time, however, if alignment is crucial to the effectiveness of cybercrime, as the advocates of the Budapest convention discuss, it is legitimate to ask whether we really have the option of choosing whether a new contract should be tried: what is the value of the Convention cybercrime if some of the countries with whose territory there is a significant part of such crime, such as Russia and China, will never sign?

Perhaps the most controversial provision of the Budapest Convention, such as Article 32, on cross-border access to stored computer data with the consent or if it is publicly available. The article reads as follows: The party may, without the consent of the other party:

a. access to publicly available (open source) stored computer data, regardless of where the data are geographically located; or

b. to access or receive, through the computer system on its territory, stored computer data located in the other Party, if the party obtains the lawful and voluntary consent of a person with the statutory authority to disclose information to a party through that computer system. Paragraph (b) of this Article is particularly a cause for concern; for Russia, this clause was in fact the main reason for her decision not to sign an agreement, because she believed that he violated the sovereignty of the country.

Boris Vasiliev of the Office of the Special Coordinator for International Information at the Russian Ministry of Foreign Affairs said: "According to the Budapest Convention, the only condition for accessing the data of citizens of other states is the permission of any other company involved in the processing." Then he explained that, in reading his country, this contributed to the practice of mass surveillance of the NSA and their colleagues. Such permission allows intelligence agencies to review and analyze Internet history in emails and track user files and transfer them to US and overseas territory, he said at a meeting.

Since then, the Council of Europe's Convention on Cybercrime has issued instructions on how to read Article 32, which explicitly contradicts this reading, particularly on two important points.

First, the Guideline explicitly states that service providers generally can not provide access to or disclose information under this provision: service providers are unlikely to be able to validly and voluntarily agree to disclose their users' information under Article 32. Usually providers will only be the carriers of such data; they will not control or own the data and therefore will not be in a position to agree.

Secondly, the article explicitly states that the article "is irrelevant to orders for domestic production or similar legal requirements within a party". Even in those rare cases where a service provider can provide access or disclosure, this provision can not be mobilized if the service provider stores data in the territory of the requesting state.

Although reading Russia could be a misinterpretation, a simple case can clearly show that the problems remain even after the clarification provided by the Guideline. What if a country hostile to India claims that a computer in India was used for a crime in that country and that its law enforcement agencies have the consent of the computer owner to access his computer and his files in India? Such a case falls into the parameters set out in the footnotes, and therefore does not require notification of the Indian law enforcement body.

Indeed, as the Guideline always emphasizes, "it is assumed that the parties to the Convention are a community of trust". But although such a presumption can work well with the relatively homogenous initiators of the Convention, it does not necessarily have to be in the world as a whole. For India, Article 32 (b) can not be a major concern as long as the other Parties to the Convention of the State with which they are friendly are concerned. Once this is changed - for example, because the country with which India has traditionally had more tense relations joins the deal - India could have justified reasons for concern.

The efforts made today to make the Second Additional Protocol to the Council of Europe Convention on Cybercrime are currently the ones that promise to reach the broader acceptable global legal norms, but the time passes will show whether this really is going to happen.

CONCLUSION

Without a common legal framework that will be globally acceptable, it is not possible to speak about legitimate data exclusion, from parts of the global Internet infrastructure, particularly those cloud types, which are physically located outside the national territories. The existing legal solutions of the national and regional levels, which are still not globally accepted, will continue to be the reason for accepting certain digital evidence in one country and rejecting it in other

countries. But without strong reasons, it will not be possible to successfully complete the process of global acceptance of a common legal framework. Following this work, there remains a challenge for the future, exploring what can be a strong enough reason to achieve global consensus over the global legal framework. Because there is no doubt that, globally, we recognize the importance of the question of lawfully excluding evidence from virtual infrastructure, which is physically located outside of our national borders and / or outside the EU.

REFERENCES

1. BBC, News: Australia data encryption laws explained, https://www.bbc.com/news/world-australia-46463029
2. Anja Kovacs: India and Budapest convention, https://internetdemocracy.in/wp-content/uploads/2016/03/Dr.-Anja-Kovacs-Inda-and-the-Budapest-Convention.pdf
3. Kristen Eichensehr: International Agreements & Disagreements on Cyber security, https://www.justsecurity.org/16706/international-agreements-and-disagreements-on-cybersecurity/
4. Paulde Hert, CihanParlar, Juraj Sajfert: The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law
5. https://www.sciencedirect.com/science/article/pii/S0267364918300207?via%3Dihub
6. U.S. Department of Justice: Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act White Paper April 2019, https://www.justice.gov/opa/press-release/file/1153446/download